European Journal of Health Law **10**: 223-237, 2003.

Privacy and the Health Information Domain: Properties, Models and Unintended Results

NICOLAS P. TERRY[1]

Introduction

Health privacy is not binary; it is difficult to find anyone who opposes the abstract concept of protecting personal health information.[2] For a non-binary issue, however, the subject is remarkably controversial. This article identifies and explores three reasons for the continuing controversy. First, the article details how privacy is only one "property" of the broad and quite complex health information domain. Second, it describes the different models available to regulators seeking to protect patient information and the operational choices made by mature regional and national legal systems. Third, the article briefly notes some of the unexpected and occasionally unwelcome results that follow from applying these protective models to the health information domain.

The Health Information Domain

The traditional and somewhat Panglossian concept of patient privacy does not fit well with the modern health information domain. As it has with other information domains, technology has dramatically changed the way patient health information can be acquired, stored, aggregated, processed, accessed and distributed. More specifically, the social, economic, and, now even, security uses[3] of health information are in almost continual tension with the domain's more patient-oriented properties.

The health information domain has several key properties that extend beyond traditional confidentiality, which is inherent in the physician-patient relationship, into the modern realm which is data protection. Individually, they are privacy,

confidentiality, anonymity, access, unity (or comprehensiveness), security, integrity and quality.

Privacy, Confidentiality & Anonymity

Traditionally, privacy and confidentiality have been used interchangeably in discussions of health information. In fact, they have diverse functions and, frequently, quite different juridical underpinnings. Confidentiality places limits on disclosure, while privacy is functionally an antecedent to confidentiality, limiting data collection. Anonymity enhances privacy by frustrating the collection of personal identifiers.

Access

Access is not a difficult concept. In practice, however, it creates immense problems because of the sheer number of persons, processes and institutions asserting access needs or "rights." The health information domain has long included the access property, establishing a multitude of public health and law enforcement exceptions to any privacy regime. Traditionally, public health provisions and those requiring access for judicial process[4] were broadly stated. In contrast, some modern public health provisions, such as those designed to combat AIDS/HIV, encourage reporting by explicitly limiting the access property.[5]

The most recent complication to the access property is the imperative to reduce medical[6] and medication[7] error. Regulators on both sides of the Atlantic have taken the position that reporting errors[8] or publicly disseminating outcome data[9] will encourage safer practices or, at least, increase consumer choice.

The access property is also being shaped by fundamental changes in the practice of medicine and shifts in the physician-patient relationship. Today, it is far more likely that a patient's care will be shared between several providers, and each will require access to a comprehensive medical record. Equally, the respect for patient autonomy, particularly choice,[10] and the responsibility for care that a patient now shares with her healthcare providers requires that a patient be given access to her own records.

Unity

The realities of modern healthcare and the evolving physician-patient relationship are changing our perception of the patient record just as they broadened the access

property. Modern, high quality healthcare requires that all information relating to a patient be contained in a single (or longitudinal) record. The implications of such a requirement, that the health information be comprehensive (and potentially include genetic data of family members) and centralized, increases the level of risk in the event of unauthorized access to an electronic health record.

Security, Integrity & Quality

The security property of the health information domain is, in essence, a correlate to the confidentiality property–essentially limiting contact with patient information to those with access rights. In practice, data security, involving both physical and electronic protections, extends considerably beyond protections provided under privacy and confidentiality systems.[11] Furthermore, providers have incentives to maintain the security of their proprietary information, information that might not otherwise be protected under privacy systems.

Data integrity goes beyond protecting against simple unauthorized access by seeking to ensure that patient information is safe against unauthorized alterations. Integrity is closely related to the broader quality property. Even though the integrity property refers to the data's quality, it does little more than apply a checksum, judging the data's quality by reference to its known and intrinsic attributes. The quality property also refers to the data's accuracy and whether the electronic patient record (EPR) is up-to-date. This quality property is in the process of expanding as external factors, such as the pervasive influence of clinical practice guidelines (CPGs) and the development of clinical decision support systems (CDSS), influence the health information domain.

These different properties of the health information domain have diverse drivers. Traditional and professional ethical constructs drive confidentiality, while self-determination and patient autonomy concepts drive privacy, anonymity, and patient access. Improving quality and accountability in healthcare delivery are dominant forces that increasingly drive access, unity and integrity. These properties are frequently in tension with one another, making the regulation of the domain particularly challenging.

Health Privacy Models

Three broad models for protecting patient health information have emerged in mature regional and national legal systems. They may be loosely described as representation-centric, collection-centric, and disclosure-centric models. These are

not mutually exclusive models, and they do not equally impact all properties in the health information domain.

A representation-centric model is not concerned with the appropriateness, effectiveness, or reach of a healthcare provider's privacy policy. Rather, it concentrates on whether the entity has declared such a policy then complies with it. The representation-centric model was the default model utilized by the world's consumer protection agencies during the infancy of e-Health and prior to the maturation of collection and disclosure models.[12]

The limitations of a representation-centric system are self-evident. Not all actors in the health information domain will express such a policy. Even published policies may not be particularly robust.[13] We should also be mindful of the language that product and service providers have historically chosen which ostensibly grants additional rights to consumers but undercuts them in practice.[14]

These concerns are alleviated only to a limited extent by the increasing interest displayed by healthcare providers in acquiring accreditation[15] or trust-marks[16] for some of their technologically-mediated activities. Applying such external standards not only increases the level of self-imposed privacy protection but also raises the likelihood that breaches of such policies will be reported. In the United States, both federal[17] and state[18] legislators have considered bills that would remove some of the voluntarism presently found in the publication of privacy policies, for example, by mandating compliance with published privacy policies (sensitive to other properties in the domain) and disclosure of breaches of privacy or security.

Mature privacy systems tend to look beyond representation-centric systems and adopt collection-centric or disclosure-centric regulation. The former applies privacy properties that restrict what data may be collected in what circumstances and by which actors. In contrast, a disclosure-centric system applies confidentiality properties, typically leaving the collection of data and possibly some of the processing unregulated.

Once a disclosure-centric model has been selected, the focus shifts to the exceptions: should the use or disclosure of information be absolutely restrained or should almost any use or disclosure be permitted if the data subject gives her consent or authorization. The US position is resolutely consent-based, even with regard to the use of medical data for marketing purposes unrelated to the patient's health. In contrast, the data directive gives to member states the option of making some data inalienable.[19]

Neither the collection-centric nor the disclosure-centric models are without problems when applied to the health information domain. For example, quality is severely compromised if the patient's data set is incomplete because of limitations on collection. Equally, applying strong disclosure-centric rules can jeopardize the access to information in shared care scenarios.

The most mature (although maturity is relative in this emerging field) systems are those of the Europe Community, the United States and Australia. As will be seen from the brief summaries that follow, Europe, at least in principal, has favored a collection-centric legislation. The United States is taking a purely disclosure-centric approach to health privacy based on a strict compliance model. On the other hand, the Australian system mixes collection-centric and disclosure-centric principles and features a particularly broad array of enforcement approaches, particularly by way of guidelines issued by its Federal Privacy Commissioner.

Europe

The standard-bearer of a collection-centric privacy model has been the 1995 European Community data directive.[20] The directive carries with it the promise of a rigorous collection-centric approach to health privacy, stating: "[P]ersonal data must be ... collected for specified, explicit and legitimate purposes."[21]

The directive also regulates the disclosure of health information, prohibiting the "processing of data concerning health ..."[22] Exceptions apply when the patient has given "explicit consent"[23] or "is physically or legally incapable of giving his consent."[24] Healthcare providers and public health authorities are given generous access to patient information.[25] The data directive provides for access and limited correction rights,[26] although these have been expanded by some member states.[27] The data directive integrates highly generalized security principles into its privacy and confidentiality scheme.[28] In contrast, the regulations made under the US Health Insurance Portability and Accountability Act of 1996 (HIPAA) will feature highly detailed requirements for physical and electronic security, training and compliance.[29]

The member states, however, have done little to promote a true collection-centric regime or meaningfully limit the disclosure of patient information within the healthcare environment. For example, the 1998 English Data Protection Act vests health information with the elevated protection classification of "sensitive personal data."[30] In the end, however, the 1998 Act operationally places few restrictions on data used in the context of the "provision of care and treatment and the management of healthcare services."[31] The UK among other European states is examining alternative protective models and has issued a consultative document on the health information domain.[32]

Given that European law has not delivered a collection-centric regime, it has not been the most successful proponent of the privacy property. In contrast, however, it is making considerable progress towards a robust anonymity construct. For example, the new data Directive on electronic communications requires non-

itemized billing, regulates caller identification options, and requires providers to anonymize global positioning-type location data.[33]

United States

America's trading partners are aware that successive US administrations have been less than forthcoming on data protection for consumers. The Clinton administration narrowly avoided a trade "war" with the EU over the extraterritorial application of the original data directive.[34] Under the Bush administration, the Federal Trade Commission (FTC) has turned its back on introducing any general privacy protection[35] and has retreated from the child online privacy rules introduced by the previous administration.[36]

With such a lackluster history, it is perhaps no surprise that the US "backed into" health privacy. Under the 1996 HIPAA Act,[37] the federal government committed to a process of "Administrative Simplification" to reduce healthcare costs. The primary component of the now infamous HIPAA initiative is the enabling of a national Electronic Data Interchange (EDI) for the US healthcare industry. An EDI vastly increases the collection and flow of patient data and thereby increasing the privacy "risk" to patients. The HIPAA statute made clear that regulatory limits would have to be placed on how far the healthcare industry could externalize these risks to patients.[38] Notwithstanding, the Standards for Privacy of Individually Identifiable Health Information[39] (PIHI), released during the final weeks of the Clinton administration but not generally applicable until early 2003, surprised many with their substantive complexity and rigorous compliance requirements. Initially, the incoming Bush administration was highly critical of the regulations.[40] This was followed by grudging acquiescence.[41] Within a year, however, the new administration promulgated, after furious lobbying by the health industry, substantial amendments to the regulations.[42] These amendments have themselves proven quite controversial, particularly the manner in which the Bush administration abandoned the requirement for consent prior to disclosure of patient data for "treatment, payment or healthcare operations" (TPO). It is possible that these amended regulations themselves will be countered with legislative action.[43]

Conceptually, the PIHI standards as they exist today are similar to the statutory controls that exist in a small minority of US states.[44] The federal rules do *not* preempt more rigorous state patient privacy protections. They are less comprehensive and considerably less comprehensible than existing state and model[45] laws largely because of the difficulties faced by the drafters in managing the limitations of the enabling legislation.[46] For example, the enabling HIPAA legislation was not written broadly enough for the PIHI regulations to apply to all "data

controllers" as seen in the Directive.[47] This created considerable problems for the US regulators seeking to protect health data that was distributed to those outside of the healthcare industry.[48] Compared to common law concepts of confidentiality and privacy and even state legislation, the PIHI regulations are ruthlessly specific, clearly preferring compliance minutiae to general statements of principle.

The PIHI regulations apply to providers such as hospitals, health insurers and physicians that "transmit any health information in electronic form in connection with a [health-EDI transaction]."[49] The regulations limit the disclosures that affected providers may make of "protected health information" (PHI);[50] a concept that in practice is functionally similar to the Directive's "personal [health] data."[51]

PIHI places no limitations on the collection of health data. It is a classic disclosure-centric system but, particularly after the Bush administration amendments, one that promises more than it delivers. First, the regulations limit use and disclosure with a "minimum necessary" rule,[52] but derogate from that rule in cases of treatment or when law requires the disclosure.[53] Second, PIHI invokes gradated levels of access permissions, dependent on the type of information utilization contemplated. These permissions include *permitted* disclosure to a broad range of public health, law enforcement, and judicial authorities as required by law and subject to various conditions[54] and *authorized* (i.e., consented-to) disclosures for other purposes such as some (and only some) forms of marketing.[55] The Bush amendments removed any requirements of consent for data used for TPO purposes.[56]

Given the highly politicized atmosphere surrounding the PIHI regulations, it is not surprising that privacy advocates have been generally protective of HIPAA. This politically-motivated support tends to distract attention from the very severe limitations in HIPAA's privacy construct. While imperfect and unnecessarily complex, the HIPAA privacy regulations *do* protect patients in many of their interactions with bricks-and-mortar providers. The same cannot be said for most consumer interactions with online providers. It is well known that health web sites on both sides of the Atlantic have failed to establish acceptable standards of data protection,[57] yet most "pure-play" e-health sites are untouched by the PIHI regulations.[58]

Australia

In Australia, both the federal (Commonwealth) and state[59] governments are aggressively pursuing the protection of patient information. The federal Privacy Act of 1988 was passed to implement OECD privacy guidelines.[60] In 2000, the Privacy Amendment (Private Sector) Act extended the operation of the Privacy Act of 1988 to cover the private sector, including healthcare.[61]

This more recent legislation introduced the so-called National Privacy Principles.[62] These principles are broadly sensitive to the needs of the health information domain and reference two protective models: collection-centric (by placing limits on collection[63] and granting consumers anonymity rights[64]) and disclosure-centric models.[65] The principles also address data quality,[66] data security,[67] and access rights.[68] The 1988 Act established the position of Federal Privacy Commissioner,[69] a position that becomes even more crucial under the 2000 Act since the Commissioner issues sector-specific privacy guidelines.[70] In late 2001, the Commissioner issued his non-binding but influential initial *Guidelines on Privacy in the Private Health Sector.*[71] To a large extent, these guidelines map the National Privacy Principles to the health context.

The Guidelines suggest a robust collection-centric approach. In most cases, consent is required prior to collecting patient health information. This consent should include disclosure of the purposes for which the information is being collected. Further, the "[i]nformation collected should be limited to what is necessary for the health service provider's functions and activities."[72]

When dealing with obligations relating to collected data, the Guidelines help distinguish between the *use* ("the handling of information within an organization") and the *disclosure* ("the transfer of information outside the organization") of patient information.[73] Specifically, the Guidelines state that a provider should "only use or disclose personal information for the primary purpose for which it was collected, or for directly related secondary purposes if these fall within the reasonable expectations of the individual ..." As a result, the Guidelines contemplate a sophisticated matrix implicating use and disclosure, primary and secondary purposes of collection, patient expectations, consent, and appropriate exceptions. Both fundraising and direct marketing to patients[74] are more constrained than under the US HIPAA regulations.

Enforcement Models

The preceding analysis has concentrated on the substantive rules protecting properties in the health information domains. An additional and extremely important variable concerns the enforcement or process model that different jurisdictions layer over a chosen substantive model.

There are five basic and seldom exclusive approaches to enforcing patient rights inherent in properties of the health information domain. First, a patient may be given a private right of action arising out of tort or warranty. Second, a legislative scheme may expressly or impliedly provide for a private remedy based on a breach of a statutory provision. Third, unauthorized collection or disclosure could lead to criminal sanctions. Fourth, those who collect healthcare information could be

subjected to detailed regulatory compliance mechanisms, breach of which may lead to administrative, civil or criminal penalties. Fifth, investigatory, enforcement and remedial powers may be granted to a discrete government or semi-autonomous agency – often called a Privacy Commissioner. Such an agency may be distinguished from traditional regulatory bodies by a high level of independence, a power to issue guidelines, and an expectation to negotiate with and mediate between industry and patient groups. No private cause of action is permitted under the US PIHI regulations. In fact, only a small number of the states that have passed their own health privacy statutes expressly allow for a private right of action.[75] Of course, plaintiffs may rely on established common law actions such as the tort of breach of confidence,[76] and, as one federal court has noted about the PIHI regulations, "the Standards indicate a strong federal policy to protect the privacy of patient medical records, and they provide guidance to the present case."[77] In accordance with the requirements of the data directive,[78] the UK Data Protection Act recognizes a private right of action for breach of the statutory duties provided for therein.[79]

The UK statute allows criminal prosecutions,[80] but its processes and sanctions are pale when compared to the compliance system envisioned by the US HIPPA regulations. No other privacy regime has adopted such detailed compliance mechanisms (including appointing a "privacy officer" and training staff in privacy compliance[81]) that underline the regulations' civil and criminal sanctions.[82]

The data directive clarified the important investigatory, adjudicatory and enforcement roles of a "supervisory authority."[83] As a result, the UK Privacy Commissioner has the power to issue enforcement and information notices. There is an appeal from such notices to an administrative tribunal and thereafter to the courts.[84] Similarly, the Australian Commissioner may make quasi-judicial determinations of privacy breaches and move for judicial enforcement.[85] Both the UK[86] (taking its cue from the data directive[87]) and the Australian[88] commissioners may encourage and then approve industry self-regulatory codes. Arguably, among the mature legal systems, the Australian Commissioner has the broadest powers and functions.[89]

Welcomed or Unintended Results

Increased regulation and enforcement within the health information domain frequently have implications beyond the properties directly targeted. For example, the practicalities of modern, high quality healthcare favor a single patient record. Equally, our conception of access includes giving a patient access to her record. This is a patient right currently recognized in the US,[90] Europe, and Australia.[91]

Irrespective of the appropriateness of such provisions, they will tend to increase the liability exposure for healthcare providers.[92]

Other implications, however, are intentional or at least welcome. Considerable indirect positives also flow from our emerging new patient information structures. Privacy was placed on the US agenda because of the need for a national health infrastructure and, therefore, a healthcare transaction EDI. That healthcare infrastructure was necessary not only to cut costs but also to improve quality.[93] Outside the US, where health privacy itself is viewed as a social good, increased regulation of the health information domain itself will act as an agent for change. As healthcare institutions upgrade their technologies to cope with increasing responsibilities flowing from privacy, security, and access provisions, those technologies and related systems will themselves enable new E-Health services. In both scenarios, improved privacy and security accelerate the utilization and acceptability of e-health business models and computer-mediated healthcare delivery.[94]

Conclusion

The *Information Strategy* of the UK NHS,[95] the *Health Online* plan of the Australian Commonwealth,[96] the *National Health Information Infrastructure* plans of the US federal government,[97] and the *eEurope-Health Online* action plan of the European Commission[98] have much in common. Notwithstanding their different structures and the distinct challenges they face, these major health systems have made it clear that the health information domain is at the core of the next generation of healthcare services.

Even this cursory analysis of the major health privacy regimes raises some challenging questions. To what extent have the architects of the mature systems taken into account the sheer complexity and multiple properties of the health information domain? What would empirical research tell us about the effectiveness and efficiency of the representation, collection, and disclosure models for protecting properties within the domain? Are there grounds for concluding that a collection-centric model is simply unworkable in a healthcare system that is prioritizing improvements in quality? How important is the substance of a protective privacy model compared to its enforcement? Answers to at least some of these questions should become available now that three influential regional and national systems have established health privacy systems that will function as complex laboratories and tell us much about how to legally shape the health information domain.

Notes:

1. Copyright © 2003 Nicolas P. Terry. All Rights Reserved. Nicolas Terry is Professor of Law & Co-Director, Center for Health Law Studies, Saint Louis University, USA. Web: http://law.slu.edu/nicolasterry Email: terry@slu.edu. Professor Terry thanks Saint Louis University health law student Trevor Wear for his research and editorial assistance.
2. See generally *A Transatlantic Perspective on Regulating Health Information*, BMJ 20 02;324:602-606 (9 March), http://bmj.com/cgi/reprint/324/7337/602.pdf
3. See e.g., Senate Blocks Privacy Project, *New York Times,* January 24, 2003 (reporting US Senate vote against Pentagon project to search for terrorists by scanning information in Internet mail and, *inter alia*, databases of health companies).
4. Cf. In re Grand Jury Investigation in New York County, 98 N.Y.2d 525, 779 N.E.2d 173, 749 N.Y.S.2d 462 (2002) (placing limits on statutory exception to physician-patient privilege that obliges hospitals and medical professionals to report gunshot and knife wounds).
5. See e.g., Doe v. Marselle, 236 Conn. 845, 675 A.2d 835 (1996) (discussing legislative reasoning behind confidentiality provisions in Connecticut's AIDS/HIV reporting statute).
6. See e.g., Janet Corrigan, Linda Kohn, and Molla Donaldson, *To Err Is Human: Building a Safer Health System* (1999).
7. See e.g., BBC News, Prescription blunders 'kill 1,200 a year' 18 December, 2001, http://news.bbc.co.uk/hi/english/health/newsid_1716000/1716130.stm.
8. See e.g., Joint Commission on Accreditation of Healthcare Organizations, Reporting of Medical Health Care Errors, http://www.jcaho.org/accredited+organizations/patient+safety/hc_errors.htm.
9. See e.g., Heart surgery deaths made public, BBC News HEALTH, Thursday, 17 January, 2002, http://news.bbc.co.uk/hi/english/health/newsid_1765000/1765692.stm; Va. Doc Site Adds Key Info, *Washington Post,* October 16, 2001; Page HE02 http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A63784-2001Oct15&notFound=true; *Sunday Times Good Hospital Guide,* January 14, 2001, http://www.sundaytimes.co.uk/news/pages/sti/2001/01/14/stipatcon01001.html#top; CMS, Nursing Home Compare http://www.medicare.gov/nhcompare/home.asp.
10. See e.g., Robert M. Veatch, *Abandoning Informed Consent,* Hastings Ctr. Rep., Mar./Apr. 1995.
11. See generally Christos Ilioudis, George Pangalos, A Framework for an Institutional High Level Security Policy for the Processing of Medical Data and their Transmission through the Internet Journal of Medical Internet Research 2001;3(2):e14, http://www.jmir.org/2001/2/e14/index.htm
12. See e.g., Eli Lilly Settles FTC Charges Concerning Security Breach, January 18, 2002, http://www.ftc.gov/opa/2002/01/elililly.htm.
13. By way of contrast consider the comprehensive voluntary policy of WebMD, of the leading health web sites, http://my.webmd.com/who_we_are/privacy/default.htm.
14. See e.g., Gladden v. Cadillac Motor Car Division, 83 N.J. 320, 416 A.2d 394 (1980) (automobile tire "warranty").
15. See e.g., URAC, http://www.urac.org/; Electronic Healthcare Network Accreditation Commission, http://www.ehnac.org/.
16. See e.g., The Health on the Net Foundation HonCode, http://www.hon.ch/HONcode/Conduct.html; Hi-Ethics, http://www.hiethics.org/.

17. See e.g., The Online Personal Privacy Act 2002 (S 2201, Sen. Hollins), http://www.techlaw-journal.com/cong107/privacy/hollings/20020418summary.asp.
18. See e.g., The Online Privacy and Disclosure Act of 2002 (AB 2297) (California).
19. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Art. 8.2(a).
20. Id. See generally Theo Hooghiemstra, Introduction to the Special Privacy Issue, *European Journal of Health Law* 9: 181-188, 2002.
21. Art. 6(1)(b). See also Art 6(1)(c), providing for an additional proportionality test and Art. 6(1)(e), essentially limiting the time data may be stored.
22. Art. 8.1.
23. Art. 8.2a.
24. Art. 8.2c.
25. Art. 8.3 ("where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.")
26. Art. 12.
27. See e.g., French Medical Records Act 2002, Loi n° 2002-303 du 4 mars 2002 art. 11-7 Journal Officiel du 5 mars 2002. See also Woman sues over mistakes in her medical records, *The Times* (London), December 2, 2002, at T2, page 10.
28. Art. 18.
29. Security and Electronic Signature Standards; Proposed Rule 63: 155 Federal Register: August 12, 1998. http://aspe.hhs.gov/admnsimp/nprm/secnprm.txt.
30. Data Protection Act 1998, s. 2 "In this Act 'sensitive personal data' means personal data consisting of information as to ... (e) his physical or mental health or condition."
31. Data Protection Act 1998, Schedules 2 and 3. See e.g., Sch 3, s. 8,
    (1) The processing is necessary for medical purposes and is undertaken by-
    (a) a health professional, or
    (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
    (2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.
32. DOH Information Policy Group, Building the Information Core: Protecting and Using Confidential Patient Information – a strategy for the NHS, 2001, http://www.doh.gov.uk/ipu/confiden/strategyv7.pdf.
33. Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37, http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.
34. See Safe Harbor Privacy Principles and other documents at http://www.ita.doc.gov/td/ecom/menu.html.
35. FTC Chairman Announces Aggressive, Pro-Consumer Privacy Agenda, October 4, 2001, http://www.ftc.gov/opa/2001/10/privacy.htm.
36. The FTC amended its own Children's Internet Privacy Rule to extend the sliding scale approach for verifying parental consent. http://www.ftc.gov/os/2002/04/67fr18818.pdf.

37. Health Insurance Portability and Accountability Act of 1996, Pub. L No. 104-191, 110 Stat. 1988 (codified as amended scattered in portions of 29 U.S.C., 42 U.S.C. and 18 U.S.C.).
38. 42 USCS § 1320d-2(d)(2).
39. 45 CFR Parts 160, 162 and 164. A consolidated version incorporating the modifications made during the Bush administration is available at http://www.hhs.gov/ocr/combinedregtext.pdf.
40. See Robert O'Harrow Jr., *Protecting Patient Data*, Wash. Post, Mar. 23, 2001, at E01.
41. Press Release, HHS Press Office, *Statement by HHS Secretary Tommy G. Thompson Regarding the Patient Privacy Rule*, Apr. 12, 2001, *available at* http://www.hhs.gov/news/press/2001pres/20010412.html
42. See HHS Press Release, HHS Issues First Major Protections for Patient Privacy, August 9, 2002, http://www.hhs.gov/news/press/2002pres/20020809a.html.
43. Statement of Senator Edward M. Kennedy, Committee on Health, Education, Labor, and Pensions, Hearing on Medical Privacy, April 16, 2002, http://labor.senate.gov/Hearings-2002/april2002/041602wit/Kennedy.pdf.
44. See e.g., Cal.Civ.Code § 56.10.
45. Uniform Health Care Information Act, Proposed Revisions 2000, http://www.law.upenn.edu/bll/ulc/uhcia/hci0600.pdf
46. See note 37, above.
47. Directive 95/46/EC Art 2(d).
48. See e.g., 45 C.F.R. § 164.504(e), dealing with 'business associate' contracts.
49. 45 C.F.R. § 160.102.
50. § 164.502(a).
51. Directive 95/46/EC Art. 2(a).
52. 45 C.F.R. § 164.502(b)(1).
53. § 164.502(b)(2).
54. § 164.512.
55. § 164.508.
56. § 164.506.
57. Consumers International, Privacy@net: An international comparative study of consumer privacy on the internet, January 2001, 5-7, http://www.consumersinternational.org/news/pressreleases/fprivreport.pdf.
58. See generally Angela Choy, Zoe Hudson, Joy Pritts and Janlori Goldman, *Exposed Online: Why the new federal health privacy regulation doesn't offer much protection to Internet users*, November 2001 http://www.healthprivacy.org/usr_doc/PIP_HPP_HealthPriv_report.pdf; Pew Internet & American Life Project, Federal health privacy regulation does not cover most Internet medical searches, services, or purchases, 11/19/01 http://www.pewinternet.org/releases/release.asp?id=33. Cf. In re Pharmatrak, 329 F.3d 9 (1st Cir. 2003) (applying the Electronic Communication Privacy Act (ECPA), the court found in favor of plaintiffs, Internet users, where they alleged defendants, a web-monitoring corporation and pharmaceutical corporations, secretly intercepted and accessed their personal information). ECPA amended the Federal Wiretap Act by extending protection to data and electronic transmissions. To have a successful cause of action under the ECPA, a plaintiff must show that "a defendant (1) intentionally (2) intercepted or endeavored to intercept ... (3) the contents of (4) an electronic communication (5) using a device. This showing is subject to certain statutory exceptions, such as consent."

59. See e.g., Victorian Health Privacy Principles extracted from the Health Records Act 2001 (Vic), http://www.health.vic.gov.au/hsc/hppextract.pdf.
60. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.
61. Effective from December 21, 2001. For the consolidated legislation see http://www.privacy.gov.au/publications/privacy88.pdf.
62. Privacy Amendment (Private Sector) Act 2000, Schedule 3, http://www.privacy.gov.au/publications/npps01.html.
63. Principles 1, http://www.privacy.gov.au/publications/npps01.html#a; 10, http://www.privacy.gov.au/publications/npps01.html#j.
64. Principle 8, http://www.privacy.gov.au/publications/npps01.html#h.
65. Principle 2, http://www.privacy.gov.au/publications/npps01.html#b.
66. Principle 3, http://www.privacy.gov.au/publications/npps01.html#c.
67. Principle 4, http://www.privacy.gov.au/publications/npps01.html#d.
68. Principle 6, http://www.privacy.gov.au/publications/npps01.html#f.
69. Consolidated Act s. 27 "Functions of Commissioner."
70. Id. pursuant to s. 27(e).
71. Office of the Federal Privacy Commissioner, Guidelines on Privacy in the Private Health Sector (October 2001), http://www.privacy.gov.au/publications/hg_01.html.
72. Id. at 1.2.
73. Id. a 2.
74. Id. at 2.3.
75. *See, e.g.*, Wis. Stat. § 146.84(c) (2001) ("An individual may bring an action to enjoin any violation of § 146.82 or 146.83 or to compel compliance with § 146.82 or 146.83 and may, in the same action, seek damages as provided in this subsection."). *See also* Cal. Civ. Code § 56.35 (West 2001); Haw. Rev. Stat. Ann. § 323(c) (Michie 2001).
76. *See, e.g.*, Hurvitz v. Hoefflin, 101 *Cal. Rptr. 2d* 558 (Cal. Ct. App. 2001); Berger v. Sonneland, 26 P.3d 257 (Wash. 2001).
77. United States v. Sutherland, 143 F. Supp. 2d 609, 612 (W.D. Va. 2001).
78. Art. 23.
79. Data Protection Act 1998 Sec. 13(1) "An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage."
80. Data Protection Act 1998 Secs. 55, 60.
81. 45 C.F.R. § 164.530.
82. 45 C.F.R. §§ 160.300-312.
83. Art. 28.
84. Data Protection Act 1998 Sec. 40 et seq.
85. Privacy Act 1988 Sec. 52 et seq.
86. Data Protection Act 1998 Sec. 51.
87. Art. 27.
88. See Privacy Act 1988 Sec. 16A. See generally http://www.privacy.gov.au/business/codes/index.html.
89. Privacy Act 1988 Sec. 27. See also Federal Privacy Commissioner, "What does the Office of the Federal Privacy Commissioner do?" http://www.privacy.gov.au/publications/pia1.html.
90. See e.g., 45 C.F.R. § 164.524(a)(1) (2001); Cal.Civ.Code § 56.07.

91. See e.g., Data Protection Act 1998 Sec. 7 (UK); Guidelines on Privacy in the Private Health Sector, 6 Access and correction (AU).
92. See generally Nicolas P. Terry, *An eHealth Diptych: The Impact of Privacy Regulation on Medical Error and Malpractice Litigation*, 27 *Am. J. Law & Med.* 361-419 (2001) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=286778.
93. Nat'l Comm. on Vital And Health Statistics, NHII Workgroup on the Nat'l Health Information Infrastructure (2000), http://ncvhs.hhs.gov/NHII2kReport.htm.
94. Nicolas P. Terry, *Structural and Legal Implications of E-Health*, 33 *J. Health L.* 605, 605 n.1 (2000).
95. http://www.doh.gov.uk/ipu/develop/index.htm .
96. http://www.health.gov.au/healthonline/.
97. http://www.nhii.org/.
98. http://europa.eu.int/information_society/topics/health/index_en.htm.